







## Article

# Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems

Iago Sestrem Ochoa <sup>1</sup> , Valderi Reis Quietinho Leithardt <sup>3,4,\*</sup> , Leonardo Calbusch <sup>1,2</sup> ,  
Juan Francisco De Paz Santana <sup>5</sup> , Wemerson Delcio Parreira <sup>1</sup>  and Laio Oriel Seman <sup>1</sup>  
and Cesar Albenes Zeferino <sup>1,\*</sup> 

- <sup>1</sup> Laboratory of Embedded and Distributed Systems, University of Vale do Itajaí, Itajaí 88302-901, Brazil; iago.ochoa@edu.univali.br (I.S.O.); leonardo.calbusch@brusque.ifc.edu.br (L.C.); parreira@univali.br (W.D.P.); laio@univali.br (L.O.S.)
- <sup>2</sup> Departamento de Informática e Redes de Computadores, Instituto Federal Catarinense (IFC), 88354-300 Brusque, Brazil
- <sup>3</sup> VALORIZA, Research Center for Endogenous Resources Valorization, Instituto Politécnico de Portalegre, 7300-555 Portalegre, Portugal
- <sup>4</sup> COPELABS, Universidade Lusófona de Humanidades e Tecnologias, 1749-024 Lisboa, Portugal
- <sup>5</sup> Expert Systems and Applications Lab, Faculty of Science, University of Salamanca, Plaza de los Caídos s/n, 37008 Salamanca, Spain; fcofids@usal.es
- \* Correspondence: valderi@ipportalegre.pt (V.R.Q.L.); zeferino@univali.br (C.A.Z.)

**Abstract:** Since the early 2000s, life in cities has changed significantly due to the Internet of Things (IoT). This concept enables developers to integrate different devices collecting, storing, and processing a large amount of data, enabling new services to improve various professional and personal activities. However, privacy issues arise with a large amount of data generated, and solutions based on blockchain technology and smart contract have been developed to address these issues. Nevertheless, several issues must still be taken into account when developing blockchain architectures aimed at the IoT scenario because security flaws still exist in smart contracts, mainly due to the lack of ease when building the code. This article presents a blockchain storage architecture focused on license plate recognition (LPR) systems for smart cities focusing on privacy, performance, and security. The proposed architecture relies on the Ethereum platform. Each smart contract matches the privacy preferences of a license plate to be anonymized through public encryption. The storage of data captured by the LPR system can only be done if the smart contract enables it. However, in the case of motivation foreseen by the legislation, a competent user can change the smart contract and enable the storage of the data captured by the LPR system. Experimental results show that the performance of the proposed architecture is satisfactory, regarding the scalability of the built private network. Furthermore, tests on our smart contract using security and structure analysis tools on the developed script demonstrate that our solution is fraud-proof. The results obtained in all experiments bring evidence that our architecture is feasible to be used in real scenarios.

**Keywords:** blockchain; Smart City; license plate recognition systems; privacy



**Citation:** Sestrem Ochoa, I.; Reis Quietinho Leithardt, V.; Calbusch, L.; De Paz Santana, J.F.; Delcio Parreira, W.; Oriel Seman, L.; Zeferino, C.A. Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. *Appl. Sci.* **2021**, *11*, 1255. <https://doi.org/10.3390/app11031255>

Academic Editor: Gabriel González  
Received: 30 October 2020  
Accepted: 20 January 2021  
Published: 29 January 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Internet of Things (IoT) has been largely employed around the world to provide a number of new services. In the IoT domain, things like everyday objects, places, and environments are interconnected with each other through the Internet [1]. This definition can serve as a basis for the design of Smart Cities. Smart cities are structures for real-time data collection and integration based on the use of sensors, applications, personal devices, and other interconnected resources [2]. When integrated into a computing platform, these features provide a set of smart services useful to solve urban problems. Such devices contribute to the sustainable development of cities and the improvement of the quality of life of their citizens.

Rjab et al. [3] have identified four primary roles of the IoT in Smart Cities: (i) ensuring the ubiquitous connectivity between different objects; (ii) collecting a large amount of data that can be analyzed, stored, and shared; (iii) improving and facilitating the accessibility of services and enabling the creation of new intelligent and personalized services; and (iv) monitoring movements in different areas of the smart city, which can improve the level of security.

Several infrastructures of a city can benefit from smart services. For instance, law enforcement organizations such as the police departments have been using license plate recognition (LPR) systems, also called license plate readers, to monitor and track vehicles circulating through the cities. As reported by the authors of [4], in 2002, police forces in England and Wales began to be equipped with LPR technology. United States (US) agencies followed suit around 2004, as did Canada and Australia. In less than one decade, LPR systems have been widely adopted by law enforcement agencies around the world as a force multiplier in law enforcement and an essential tool for fighting crime. LPR systems take photographs of vehicles and, through image recognition technologies, collect and store the license plate number, date, time, and location of each reading. Law enforcement organizations use these data to detect stolen vehicles, identify, and monitor suspect vehicles, or even wanted individuals.

Concern has raised from the use of LPR systems based on the privacy of the captured data [5]. LPR systems do not distinguish between vehicles under criminal investigation and those that are not. This feature violates the data protection laws in countries that protect the storage of personal data without consent or motivation provided by law. Organizations that use LPR systems have faced questions from citizens and organizations that defend the privacy of individuals. The captured image of a vehicle, its license plate, location, and the date and time the image was recorded provide a basis for inferring personal characteristics about the driver. Therefore, it is clear the need for solutions to protect privacy in cities that use LPR systems for vehicle monitoring. These systems must be implemented considering guarantees of privacy of the data they capture, not allowing that data to be stored and processed in disagreement with the provisions of the current data protection laws.

Based on a systematic literature review, we have identified a lack of solutions to guarantee privacy in LPR systems. Given this gap, in [6], we presented a proposal of a storage architecture that uses blockchain technology to guarantee the privacy of data captured by LPR systems. This architecture relies on the Ethereum platform, a decentralized network capable of executing smart contracts. In our model, each smart contract will match the privacy preferences of a license plate that will be anonymized through public encryption. Thus, the storage of data captured by the LPR system cannot be accomplished if privacy protection is enabled in the smart contract associated with the license plate. Our architecture uses a gateway to control access to the blockchain smart contracts. In case of motivation foreseen by the legislation, the smart contract associated with a specific license plate can be changed by a competent user to allow the storage of the data captured by the LPR system.

In this article, we build on our previous work [6] and delve deeper into the description and evaluation of the proposed solution, presenting new results that contribute to the objective of the work. We discuss in more detail the characteristics and limitations of solutions presented in the literature to provide privacy in IoT systems that use blockchain technology, the basis of our solution. We also deepen the performance evaluation experiments, bringing more evidence about the viability and limitations of our solution. We evaluate the cost of building the smart contract developed, the number of contracts that can be stored per block, and the time to register and retrieve contracts on the blockchain. Besides, we introduce a security evaluation of the smart contracts implemented, a kind of analysis that we did not find in the works reported in the related work evaluated in our study. This security analysis relies on the main current flaws and bugs of the Ethereum platform. The results obtained in all experiments bring evidence that our architecture is feasible to be used in real scenarios.

As the main contribution, this work presents a detailed description and evaluation of the performance and security of a storage architecture based on blockchain for protecting the privacy of users of LPR systems. Furthermore, the architecture presented can be adapted to other environments that need privacy, security, and trust in IoT scenarios. Concerning our previous paper, this work introduces the structural security analysis of the smart contract. In [6], we conducted a performance analysis of the proposed architecture, evaluating response time for key recovery, cost of developing contracts, and execution time. In the current work, we seek to evaluate the security of the developed contract considering that it has a simple structure in relation to other smart contracts. Taking this into account, the additional contributions of this work are listed below.

- (i) The structural security analysis of the contract developed using Surya and Mytril tools to identify flaws and bugs in the developed smart contract.
- (ii) The security tests based on Reentrancy, Front-Running, and Gas Limit Denial of Service (DoS) attacks in the contract developed to identify security flaws in the contract code.

The remainder of this paper is organized as follows. Section 2 presents the theoretical basis on which this work was based, discusses the operation of LPR systems and the current scenario of adoption of these systems around the world, and ponders about data protection legislation in different countries. In Section 3, an analysis is conducted regarding the use of blockchain to ensure privacy in IoT environments. Section 4 describes the architecture proposed to solve the privacy problem of the chosen scenario. Section 5 discusses the results obtained from experiments conducted to evaluate the performance of the proposed architecture. Section 6 presents the results of the security tests executed on the implemented smart contract. Finally, Section 7 presents the conclusions and discusses future work.

## 2. Background

This section presents the definition of LPR systems and the current state of their adoption in some countries. We highlight the benefits of its application in the field of public safety and the impact on the privacy of monitored individuals. We also review data protection laws that aim at ensuring the privacy of individuals about the storage and processing of personal data, demonstrating how LPR systems pose threats to privacy.

### 2.1. LPR Systems

LPR systems are automatic image processing systems that recognize the license plate number of a vehicle. Such systems work on one or more camera-taken pictures that may be of the color, black-and-white, or infrared type [7]. LPR systems combine several techniques to obtain the license identifier, such as object detection, image processing, and pattern recognition. After the license plate number is obtained, it can be associated with data stored in databases, and this crossing of information enables other analyses for a diversity of applications. Examples include electronic payment systems (toll payment, parking fee payment), monitoring systems that identify road traffic intensity, and surveillance and monitoring of individuals and vehicles [4,7].

When an LPR system detects a vehicle and recognizes its license plate number, this number is compared to vehicle database records of interest in criminal investigations. In the case of a suspect vehicle is identified, a law enforcement officer can intercept and stop the vehicle, check for evidence, and, whether necessary, make arrests. However, all the license plate numbers of vehicles passing through a camera are stored, even the ones of non-suspect vehicles [8]. As the LPR system of a city can recognize and register hundreds of license plate numbers every minute, it stores large amounts of data. These data are stored for a period for use in future investigations (the legislation of each country determines this period). Thus, when a vehicle of interest is registered in the system, the authority can perform retrospective analysis and identify possible locations of an investigated suspect based on the movement history of his/her vehicle.

The storage of data regarding vehicles that are not of investigative interest has raised concerns about the privacy of citizens. On the one hand, police forces around the world claim that the use of LPR systems has increased the power of crime prevention and aided investigations. On the other hand, civic organizations and ordinary citizens have questioned whether LPR systems protect the personal data associated with the identified license plates. They worry that such information could be used for purposes unrelated to public safety. In any case, the use of LPR systems by police forces has increased significantly around the world, under different justifications [9].

According to the authors of [4], the first adherents of LPR systems were the police departments and government agencies of the United Kingdom (UK), around 2002. Then, the UK Home Office, a ministerial department of Her Majesty's Government of the United Kingdom responsible for immigration, security, and law and order, began to build and evaluate strategies for using LPR systems. Research indicates that, by 2006, all police forces in England and Wales had LPR technology. Over the same period, many similar technologies related to vehicle traffic monitoring were already available, including radar and traffic light cameras, as well as toll cameras. UK law enforcement agencies use LPR systems within a nationally interconnected infrastructure that centralizes the storage of captured data in a single data center, which is governed by standards for the use of technology [10].

In the United States, LPR systems were introduced around 2004 and quickly gained popularity in law enforcement circles. In 2007, the International Association of Chiefs of Police (IACP) established a resolution promoting the use and purchase of an LPR system with federal funds [11]. At that time, a survey conducted by the US Department of Justice estimated that about 19% of agencies with more than 100 employees were using LPR [12] systems. A survey published in 2013 shows that this percentage increased to 66% in that year [13]. A new research was conducted in 2016, but until this moment (2020), the results of this research had not yet been disclosed.

## 2.2. The Privacy Problem

The expansion of LPR systems usage has raised questions about protecting the privacy of citizens because such systems enables the monitoring of any vehicle identified. Several organizations and news agencies have been concerned about these issues.

The EFF (Electronic Frontier Foundation), a nonprofit organization based in San Francisco, California (CA), working on digital rights advocacy, requested information regarding the use of LPRs in the United States. Utilizing the transparency law, they assessed that LPR systems from 2016 and 2017 performed more than 2.5 billion license plate recognitions. Furthermore, according to the study, 99.5% of the monitored vehicles were not associated with criminal investigations [14].

According to the authors of [15], police agencies or private corporations that collect and store vehicular license plate data could track the location of a vehicle by inferring a wide range of information about private life, history, religion, or personal beliefs of an individual.

Two of the most critical aspects of privacy concerning data captured by LPR systems are the life-time of the records in the LPR database and the control access to the database. The concern for privacy primarily focuses on readings maintained in the LPRs database that were not associated with activities of interest to the police when they occurred. These records can be explored later, at the discretion of who owns the property and access to the database because, in most cases, LPR systems are sold to government institutions by private companies, and it is unclear to what kind of use such data may be susceptible.

Nevertheless, each country has different laws protecting the privacy of its citizens. In general, these laws protect the citizen against the storage of personal data captured without explicit consent. Some exceptions are allowed, such as the storage of personal data by public interest, public security, and others. The problem is compliance with these laws

by the technologies employed in the LPR systems in use today. In the system proposed in this article, we meet these requirements to offer a solution that fits most countries possible.

### 2.3. Legislation

Dozens of countries in the world already have specific legislation for data protection. In May 2018, the GDPR (General Data Protection Regulation), a data protection law approved since 2016 [16], became applicable in the European Union (EU). In the United States, data protection takes place through a set of federal and state laws, making the handling of data privacy issues vary from state to state.

The European Parliament adopted the GDPR in April 2016. The law is an evolution of the 1995 European Directive (Directive 95/46/EC) and came into force after a transitional period of two years, on 25 May 2018 [16]. The law applies not only to organizations located within the EU but also to all companies which process and hold the personal data of data holders residing in the EU irrespective of the location of the company. Organizations can be fined up to 4% of their annual global turnover for violating GDPR, and the fine can be up to 20 million euros. This fine is the maximum penalty that can be imposed for more serious infringements, such as not having sufficient consent of a customer to process his/her data.

The new European law reinforced the conditions of consent. The request for consent must be filled out in an intelligible and easily accessible form, and the purpose of processing the personal data of a client must be attached to that request. Consent should be explicit and distinguishable from other subjects, using language that is easy to understand. Moreover, it should also be easy for the client to withdraw their consent at any time. Explicit consent is required for the processing of confidential personal data. The client must register his/her option for the consent of the use of his/her data. However, for non-sensitive data, “unambiguous” consent is sufficient. In other words, the provision of data is enough to be considered that the consent is implied, even whether the client does not register the consent option explicitly. An example of “unambiguous” consent is providing an email address for receiving news from a website.

GDPR provides some exceptions to the need for consent to personal data, such as in matters relating to national security, defense, and public safety [17]. In addition to these exceptions, we should highlight the provision in the law of excluding the need for consent in cases involving the prevention, investigation, detection or prosecution of criminal offenses, or the execution of criminal sanctions aimed at safeguarding against threats to public security and prevention.

Unlike the EU, the United States follows a sector-wide approach to data privacy protection. There is no comprehensive federal law that guarantees the privacy and protection of personal data. Instead, legislation at the federal level primarily protects data within industry-specific contexts. Personal data protection in the country depends on federal and state laws, administrative regulations, and specific self-regulatory guidelines. The privacy protection guarantees are specific for each state and are located in a wide range of legislative instruments and jurisprudence [18].

Many statewide laws regulate the collection and use of personal data in the United States, and the number grows each year. On 28 March 2018, all 50 states and the District of Columbia, Puerto Rico, and the US Virgin Islands enacted laws requiring notification of security breaches involving personal information. As technological threats evolve, US legislation is progressing, and soon it is likely to establish more comprehensive legislation at the federal level, such as the European GDPR.

In one case in the state of Virginia, USA, a citizen contested the collection of his data at the LPR system of the Fairfax County Police Department (FCPD) [19]. The claim was based on a state privacy law called the “Government Data Collection and Dissemination Act”, which states that personal information “will not be collected” by state agencies “unless the need has been clearly established in advance”. The Virginia court has ruled that the vehicle data collection of the FCPD is not exempt from the law’s requirements of this law. Virginia law defines “personal information” as including “all information that provides a



basis for inferring personal characteristics". Based on this definition, the Fairfax County court decided, in April 2018, images and associated data stored in the LPR database of the FCPD meet the statutory definition of "personal information". Virginia law provides that authorities can process personal information on investigations and information collection related to criminal activity. However, according to the finding of the Court, the "passive use" of LPR systems by the Police Department does not fall within this exception and therefore is not exempt from the operation of the Data Law. The Court ceases its conclusion by justifying that the FCPD collects and retains personal information without any suspicion of criminal activity at any level of abstraction. In doing so, it has created an information system that deals with investigations and collection of information that are not related to criminal activities.

#### 2.4. Pseudonymization

GDPR refers to the term *pseudonymization* as a principle to protect personal data. It defines the term as the processing of personal data in such a way that the data can no longer be assigned to a specific Data Subject without the use of additional information. In other words, pseudonymization is the treatment by which a data loses the possibility of an association, directly or indirectly, to an individual, but by the use of additional information maintained separately by the controller in a controlled and safe environment.

When data is transformed into a pseudo-animated form, it is impossible to use it directly to identify a person. The possible method of meeting the GDPR request is encryption, in which the data being encrypted ceases to be readable directly and can be read only by a key or a pair of security keys.

In this context, blockchain technology presents itself as a viable solution to the problem above, as its principles rely on the intensive use of cryptography, a key feature of blockchain networks, in addition to bringing reliability behind all the interactions in the network. Smart contracts—automatic execution scripts residing in the blockchain—integrate these concepts and allow distributed, highly automated workflows [20].

#### 2.5. Blockchain

The blockchain concept was proposed in [21] and introduced in 2008 through the bitcoin currency. This application demonstrated the ability of the bitcoin technology to guarantee integrity in point-to-point transactions without the need for third-party auditing. Besides, the blockchain also guarantees security and privacy in the transactions carried out.

Blockchain is a data structure in which the blocks are linked together, forming a chain. Information is stored within each block, and this information may vary for each blockchain. The blocks are connected using a cryptographic hash function. Over the years, several blockchains have been created to satisfy specific operating conditions, and the Ethereum network is one of them.

Ethereum is a platform capable of executing smart contracts and storing them on its blockchain. The contracts executed on the Ethereum platform are immutable; that is, they work as scheduled without any possibility of alteration by unauthorized users in its code after its creation.

Smart contracts are scripts stored on the blockchain. They can be considered analogous to the procedures stored in relational database management systems; that is, they are automatically triggered after a transaction is triggered. They reside on the blockchain and have a unique address. In [20], the authors explain that a smart contract is triggered when addressing a transaction to it. It is then executed independently and automatically in a prescribed manner on all nodes in the network, according to the data in the triggering transaction. The authors point out that smart contracts enable managing data-driven interactions between entities on the network, establishing rules of interaction that cannot be circumvented.

### 3. Related Work

Ochôa et al. [6] propose an architecture focused on privacy in LPR systems. The central premise of the architecture proposed by the authors is that the user is the one who decides when he/she wants to be monitored, and this rule can be changed only with a court order from the competent authorities. As a solution, the authors propose a smart contract that stores the privacy preferences of the user. Asymmetric cryptography is used with the contract to guarantee the anonymity of the entities present in the architecture. This work is an evolution of the architecture presented by Ochôa et al. [6], by assessing the security level of the smart contract developed, as it is shown in the last column (SSC) of Table 1.

When performing a systematic literature review to identify other works proposing the use of blockchain for LPR systems, the results of this review pointed to the lack of such studies. In this sense, this section gives a brief review of other IoT applications. The summary of the identified works is presented in Table 1.

**Table 1.** Comparison and characterization of related work on privacy in IoT environments.

Work	SC	E	A	BC	SSC
Yu et al. [22]	•			•	
Pouraghily et al. [23]	•	•			
Rifi et al. [24]	•				
Cha et al. [25]	•				
Pinno et al. [26]				•	
Huang et al. [27]	•		•		
Dang and Nguyen [28]	•				
Ayoade et al. [29]	•				
Paul et al. [30]		•		•	
Gallo et al. [31]	•			•	
Le and Mutka [32]			•	•	
Liang et al. [33]		•			
Dorri et al. [34]		•		•	
Wang et al. [35]			•	•	
Ali et al. [36]				•	
Chanson et al. [37]		•			
Laszka et al. [38]			•		
Le et al. [39]		•	•	•	
Loukil et al. [40]	•				
Yang et al. [41]	•				
Ochoa et al. [6]	•	•	•	•	
This work	•	•	•	•	•

Note: SC: Uses Smart Contract; E: Applies encryption; A: Employs anonymization; BC: Uses Blockchain; SSC: Evaluates the security of the smart contract.

From Table 1, it can be seen that no work other than [6] was identified to employ—in the same application—smart contracts, encryption, anonymization, and blockchains. Table 1 summarizes and compares the main features observed in the literature review. The SC column identifies whether the solution proposed uses smart contracts to provide privacy. As we can see, this approach is employed by around 50% of the authors. These works use smart contracts to store the privacy preferences of the users or to provide access control to the information. The E column identifies the works that adopted encryption techniques to improve user privacy. If we do not consider this article and our previous work [6], we observe that few works (only six) employed encryption to manage data privacy with the use of public keys to identify the entities present in each architecture. The next column (A) marks the works that applied anonymization techniques to provide privacy to the users, ensuring that his/her data could not be traced/mapped. As before, few studies (only five) use this technique to anonymize the users' identity, making it impossible to identify them. Following, BC indicates the works that chose to use private and consortium blockchains

in their architectures. Half of the works used this solution to eliminate computational overhead and ensure privacy so that only specific users could access the data stored in the blockchain. Many of the works above integrate the techniques discussed to guarantee security in their architectures. However, none of them evaluate the security level of their smart contracts (when used). It is worth noting that most of the works integrated at least more than one technique to guarantee the security and privacy in their architectures.

On the other hand, it is important to notice that there are works on the literature dealing with vehicle plate identification using technologies not listed above. For instance, Andreica and Groza [42] experiment the use of the license to identify vehicles and use this identification number to bootstrap security based on identity-based cryptography schemes. In this sense, they performed experiments with Android smartphones in order to determine the feasibility of the solution. From the results, identification based on license plate number can be done with high accuracy at a range of around 50 m.

#### 4. Architecture

Security and privacy are important factors to be considered when developing IoT architectures that use Big Data [43]. In light of this, we chose to apply all the technologies discussed above (smart contracts, encryption, anonymization, and blockchain) to obtain a high level of privacy for the users. This section presents our proposed architecture.

##### 4.1. Premises and Requirements

The first premise of our system is that a user should not be monitored when he/she does not want to. Nevertheless, as a second premise, we consider that the legislation of each country/state establishes the conditions for monitoring a person at a particular moment. Based on these premises, our architecture addresses three points (requirements):

1. An individual who does not want to be monitored will not be monitored unless the government has a legal order for that.
2. The government can monitor an individual. However, at the end of the investigation process, he/she should be alerted about this monitoring.
3. An individual can be monitored and be aware of that if it is necessary (e.g., monitoring of people on probation).

In order to fulfill the requirements above, we use all the techniques listed in Table 1, as follows.

##### 4.2. Technologies

Our architecture integrates the following four architectures:

###### 4.2.1. Smart Contracts

Our architecture uses smart contracts to store the privacy preferences of a user, which can choose to be monitored or not. If it is necessary to monitor a user (e.g., the government acquires a court order authorizing the monitoring), the privacy preferences of the contract are changed, enabling the monitoring of the license plates.

###### 4.2.2. Encryption

Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data, which has been widely used due to its security level and reduced key sizes when compared to other algorithms (e.g., Rivest, Shamir, and Adleman—RSA), see [44] for an overview. We applied ECC to generate the cryptographic keys, with a pair of public and private keys generated for each system's user; the public key is used for encryption/decryption of a legal order. Any governmental agency wishing to monitor a user must also have a pair of public/private keys and use the public key to identify a governmental representative's access to the license plate database.



#### 4.2.3. Anonymity

As far as anonymity is concerned, the use of public keys will also serve as a pseudonym and will consequently make all users anonymous. This approach is adopted because with a public key, even though it is distributed on the network, only the owner of the license plate will know the key that corresponds to his/her license plate. Note that there is no exchange of messages between users under monitoring. Information exchange only happens between the monitored user and the governmental agency.

#### 4.2.4. Private Blockchain

To eliminate the existing computational overhead, we decided to use a private blockchain. Even choosing this type of blockchain, the smart contracts also ensure that the system is immutable as the conditions stored in the contracts cannot be changed. Note that users will not have access to the blockchain, only the government. In this way, the user will know that he/she is under monitoring through a notification sent by the gateway in a proper time.

#### 4.3. Scenarios

Based on the information presented, we designed our architecture by addressing the three requirements mentioned at the beginning of this section. Our architecture relies on the scenario illustrated in Figure 1, which is described below.

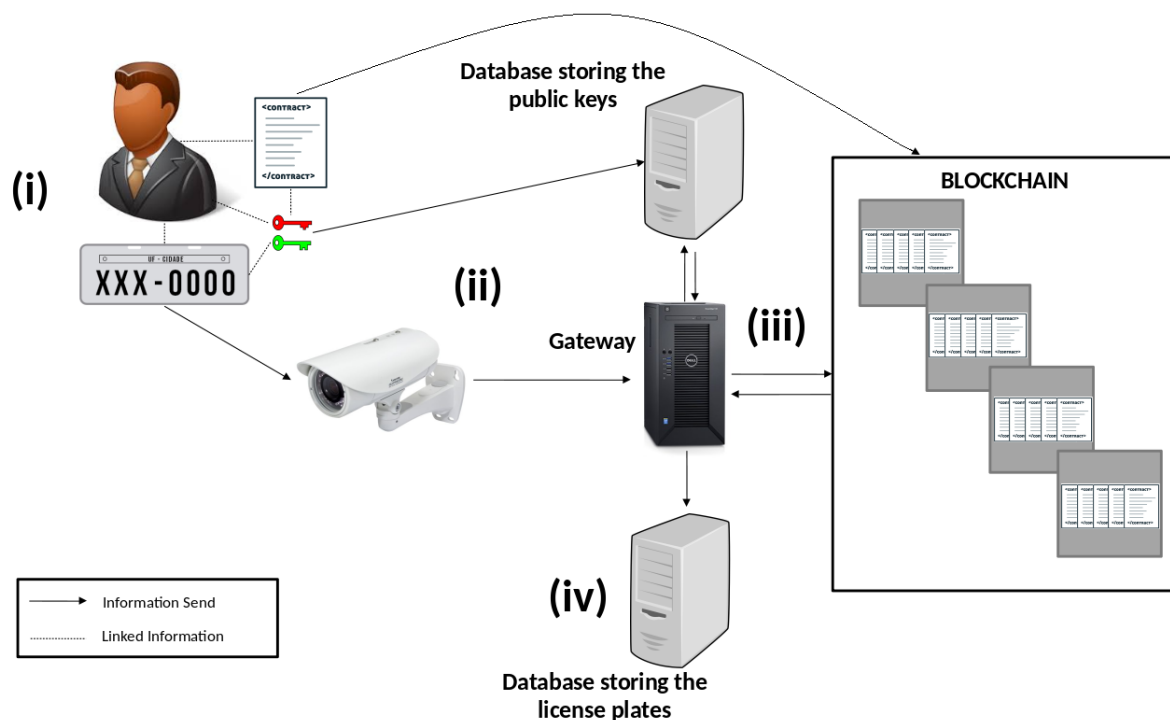
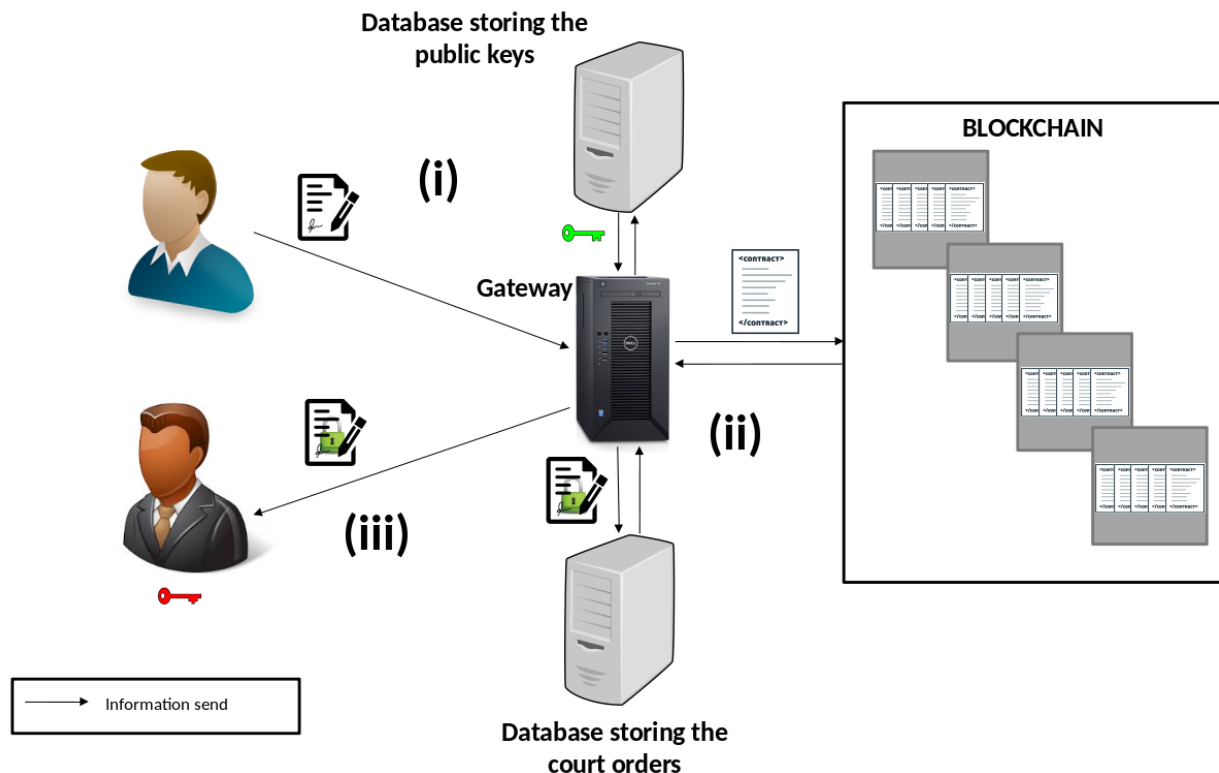


Figure 1. Proposed architecture.

- (i) The user requires the license plate for his/her vehicle and configures the privacy preferences for monitoring. This information is registered in a smart contract stored in the private blockchain. At this point, the public and private keys of the user are also generated. When the user requires the license plate, the registration is done by a system connected directly to the blockchain, without going through the gateway. Moreover, only the authorized addresses can change the privacy preferences of a smart contract after it is registered.
- (ii) When the license plate is captured by an license plate recognition (LPR) system, the captured image is sent to the gateway responsible for managing all communications.

- The gateway connects to the database that has stored the public keys corresponding to each license plate and retrieves the corresponding public key.
- (iii) After retrieving the public key, the gateway connects to the blockchain and checks the privacy preferences of the captured license plate through the smart contract.
  - (iv) If the privacy preference of this license plate allows the image to be captured, the gateway stores its image in a storage service. On the other hand, if the user's preferences forbid the license plate capture, no image is stored.

Figure 2 illustrates the scenario used when it is necessary to monitor an individual, as described below.



**Figure 2.** Architecture for monitoring an user for a specified time.

- (i) To initiate the monitoring process, the government user must obtain a court order authorizing the monitoring. The court order must be sent to the gateway.
- (ii) The order is encrypted using the license plate owner public key, and the smart contract privacy preferences are changed, allowing the license plate to be monitored for a certain time.
- (iii) Upon completion of the monitoring time, the encrypted court order is sent to the user stating that he/she has been monitored with an order. When the monitoring time ends, the contract privacy preferences are updated to the original settings.

## 5. Performance Evaluation

This section presents an analysis of performance based on a set experiments carried out to verify the feasibility of the proposed architecture.

### 5.1. Recovery of the Public Key

The first test aimed at identifying the time it takes to retrieve the public key of a user by connecting the gateway to the database, as shown in Figure 2. In the experiments, we have used PostgreSQL 9.4 database system, running on a host computer with Debian 9.8 OS, 4 GB of RAM, and Intel Core I5 1.6 GHz processor. The gateway was running on

another computer running Ubuntu 18.04 LTS with 8 GB of RAM and Intel Core I5 2.3 GHz processor. We have measured the time to fetch 1, 10, 100, and 1000 keys at a time, using three database sizes: 100,000, 1 million, and 10 million license plates. Table 2 summarizes the query execution time to retrieve a given number of keys for each database size. We can observe that the execution time of the queries varies according to the number of keys retrieved and also with the database size. It is worth noting that the higher number of license plates stored in the database is less the number of vehicle plates licensed in cities like New York, which do not reach the amount of 10 million private cars [45].

**Table 2.** Key recovery query execution time varying database size.

Keys Recovery/DB Size	100 K	1 KK	10 KK
1	1.57 ms	1.60 ms	1.66 ms
10	1.68 ms	2.09 ms	1.91 ms
100	1.80 ms	7.13 ms	9.18 ms
1000	4.12 ms	10.03 ms	12.05 ms

### 5.2. Smart Contract Cost

We used Ganache and Truffle to implement a private blockchain and develop the contracts. Ganache is a personal Ethereum blockchain which enables developers to create smart contracts, dApps, and test software, and inspect state while controlling how the chain operates. Truffle is a development environment, testing framework and asset pipeline for blockchains based on the Ethereum Virtual Machine (EVM). The first point observed during the building of the network was the limit amount of gas for each block. By default, Ganache uses blocks of 6,721,975 gas, while Main-net currently uses blocks of 8,000,000 gas. To set the limit amount of gas per block on our blockchain, we first verified the gas cost of the smart contract developed.

As we can see in the algorithm shown in Figure 3, the system performs an address mapping that can change the privacy preferences of a contract. If the gateway verifies that the contract does not include the requestor address, it cannot be changed. We consider that one or more government agencies can request monitoring, and therefore each agency must have a registered address.

```

1  pragma solidity 0.6.4;
2  contract PrivacyPreference {
3      bool private preference = false;
4      bool private monitoringType = false;
5      mapping (address => bool) private addresses;
6
7      constructor () public {
8          addresses [address(0x00281055afc982d96fab65b3a49cac8b878184cb16)] = true;
9      }
10
11     function changePreferences() public {
12         if (addresses [msg.sender])
13             preference = true;
14     }
15
16     function changeMonitoringType () public {
17         if (addresses [msg.sender])
18             monitoringType = true;
19     }
20
21     function preferenceStatus() public view returns (bool) {
22         return preference;
23     }
24
25     function monitoringStatus() public view returns (bool) {
26         return monitoringType;
27     }
28 }

```

**Figure 3.** Privacy preference smart contract.

A smart contract consumes an amount of gas to be stored into the Ethereum blockchain. To assess the gas cost of each contract, we performed experiments by varying the number of

addresses authorized to change the privacy preferences of each user. The results obtained are shown in Table 3. As we can observe, the gas cost increases with the number of addresses mapped in the contract. As the Ethereum network becomes expensive to store values, we chose to use ten addresses for each contract.

**Table 3.** Gas cost varying the address quantity.

Addresses	Gas Cost
1	173,833 gas
10	300,290 gas
100	1,324,958 gas

Based on the value obtained in the previous experiment, we set the limit amount of gas for each block to store 20 contracts. Table 4 presents the comparison of contracts stored in our network with Main-net and the standard Ganache network. The results show a small difference between the number of contracts stored in our network with Main-net and Ganache. This difference does not change the operation of the network compared to Main-net as the gas size of each block in Main-net varies over time.

**Table 4.** Contracts stored by block in different networks.

Network	Contracts Stored
Default Ganache	22
Ethereum Main-net	26
Our Network	20

In our network, we set the limit amount of 6,005,800 gas per block, enabling the storage of exactly 20 contracts per block, considering the structure shown in Figure 3. This value does not compromise the network performance because we use a private blockchain.

### 5.3. Registration and Verification of Contracts

Considering that each registered license plate corresponds to a contract, we evaluated the registration time of contracts in our blockchain through the gateway. For this experiment, we hosted our blockchain on a machine running Ubuntu 18.04 LTS with 2 GB of RAM and Intel Core i7 3.8 GHz processor. We then used the web3.js library to register and verify the contracts by establishing a connection with the blockchain. Following, we measured the execution time for the registration of 1, 10, and 100 contracts. Table 5 presents the results obtained. From these results, we observe that the time necessary to register transactions in blockchain varies linearly with the number of contracts being registered concurrently.

**Table 5.** Execution time for contract registry in blockchain.

Contracts	Execution Time
1	0.52 s
10	4.20 s
100	38.35 s

Next, we used the address of each contract generated to perform its search in the blockchain and evaluate the connection time of the gateway with the blockchain. We dismissed the time the gateway takes to obtain the contract address from the database. As the results presented in Table 6 show, the increase in the number of blocks has minimal impact on the time for obtaining a contract stored on the blockchain.

**Table 6.** Execution time to obtain a contract in blockchain.

Blocks	Execution Time
1	0.43 s
10	0.45 s
100	0.46 s

Based on the results obtained from the experiments presented above, we consider that our architecture can be employed in real-world systems. However, it is worth noting that we did not perform database scalability tests on a real system, and several aspects still need to be analyzed. For instance, registering the same vehicle as it travels through the city requires a strategy to reduce storage costs. Furthermore, the database scalability depends on the number of capture points, the resolution of the images, and the additional information to be stored. The system's scalability also depends on its ability to meet the time requirements for registering multiple images captured by the multiple cameras of one or more cities served by the system. These aspects will be investigated in future works that involve applying the proposed solution in a real system.

## 6. Security Evaluation

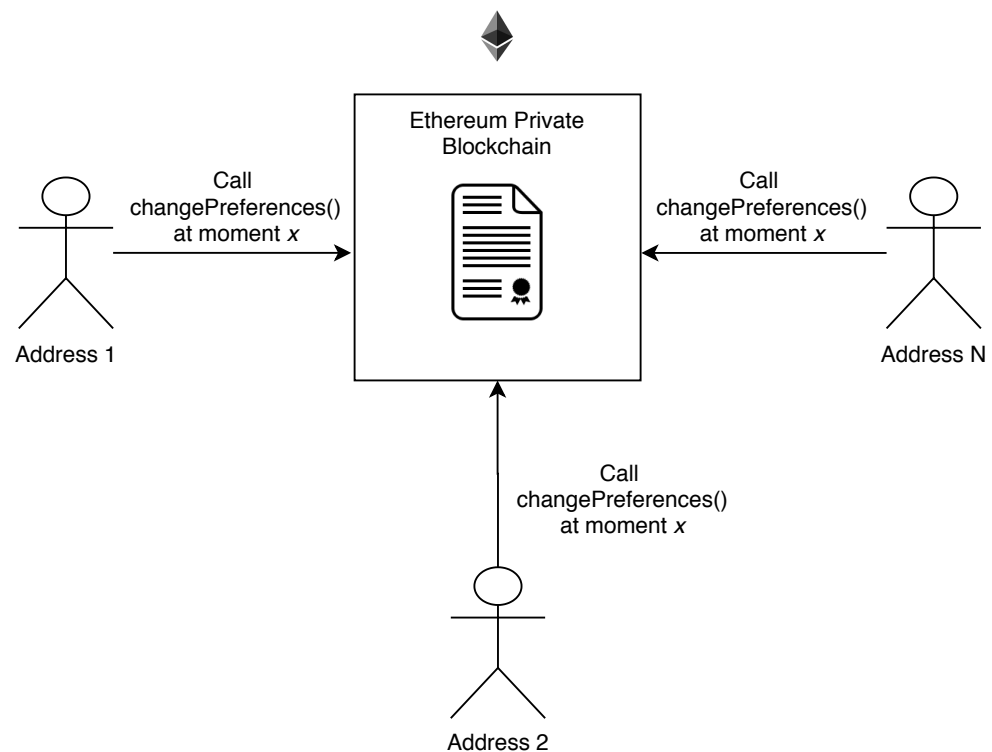
In this section, we seek to assess the security of the developed smart contract. In this evaluation, we employ a methodology to identify the main types of attack which can be carried out in smart contracts [46]. Among them, we identified three possible attacks to our contract:

1. *Reentrancy*: The repeated call of a smart contract function by different users can lead to an inconsistency in the final result of the function. In order to evaluate this attack in our contract, we chose to invoke the `changePreferences` function for  $n$  different users.
2. *Front-running*: A `changePreference()` transaction can be seen in the mempool (i.e., the memory pool) of the platform before it is executed, and a person can react in advance before that transaction is processed. The memory pool has the function of storing unconfirmed transactions. Once a transaction is generated, it is transmitted to the network and stored in the mempool [47]. In our tests, we seek to observe the behavior of several transactions in the mempool.
3. *Gas Limit DoS*: A transaction can be denied when a user invokes one or more transactions trying to exceed the gas limit of a block, so the transaction is not processed. In our tests, we seek to generate an exploit in the contract trying to exceed the gas limit.

To carry out the first type of attack (Reentrancy), we chose to call the `changePreferences()` function simultaneously from different addresses on the blockchain. For that, we registered in the smart contract the addresses that could have access to the blockchain. As previously defined, the maximum number of addresses stored in a contract equals 10, so the test developed was limited to this value. Figure 4 illustrates scenario used. In this test, we verify whether the flow of calls to a specific function of the contract can generate inconsistencies in it.

As can be seen in Table 7, according to the results obtained, the contract developed was not influenced by the Reentrancy attack. We noticed that the attack was not effective due to the simplicity of the `changePreferences()` function. Contracts with higher complexity could be affected by this attack.





**Figure 4.** Reentrancy attack model.

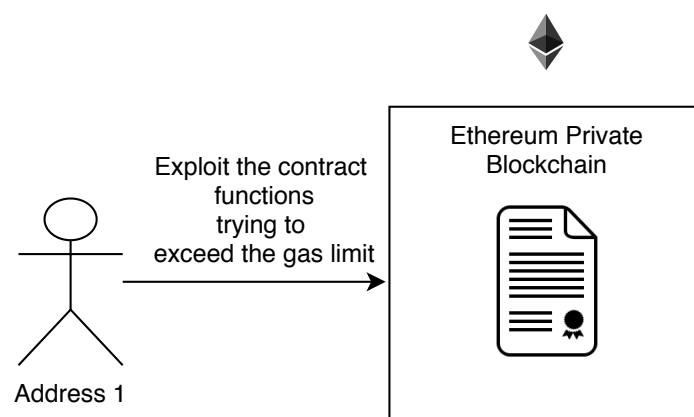
**Table 7.** Reentrancy attack result varying the number of addresses.

Addresses	Expected Result	Final Result
2	True	True
5	False	False
10	True	True

To carry out the Front-Running attack, we observed the mempool of the transactions in Truffle Console and used the `changeMonitoringType()` function to perform this test. After calling the function, we sought to identify the blockchain transaction in the mempool. However, as we use a private blockchain and few transactions, the function was processed at the time it was called. As such, there was no time to process another transaction before it had been processed. Another cause of this effect was the simplicity of the contract developed. Figure 5 presents a screenshot from the console of the environment used in which we can see that a new block was created at the time of calling the `changeMonitoringType()` function. The `logsBloom` shown in the figure is the Bloom filter record, which aims to preserve the user's privacy and resist third-party attacks.

In the third test (Gas Limit DoS), we explored the contract to generate a denial of service attacks. For this test, we used both the functions available in the contract. Figure 6 illustrates the scenario used in the test. As we can see, unlike the first attack, this test attempts to generate an exploit in the contract to exceed the gas limit of the block. This type of attack allows a transaction not to be processed, unlike the Reentrancy attack that seeks to maliciously change the value of a transaction using an exploit without exceeding the gas limit of the block.

**Figure 5.** Truffle console showing the processed transactions.



**Figure 6.** Gas Limit Denial of Service attack model.

From the tests performed, we realized that the contract developed is tamper-proof from Gas Limit DoS. Again, due to the simplicity of the smart contract, when a function is called multiple times, it is processed instantly, not allowing DoS attacks. However, we realized that the complexity of the algorithm directly influences this security issue. The complexity of the developed algorithm is classified as  $O(1)$ , which makes the attack impossible. Table 8 presents the probability of a DoS attack occurring according to the complexity of the algorithm when the contract design is not done correctly.

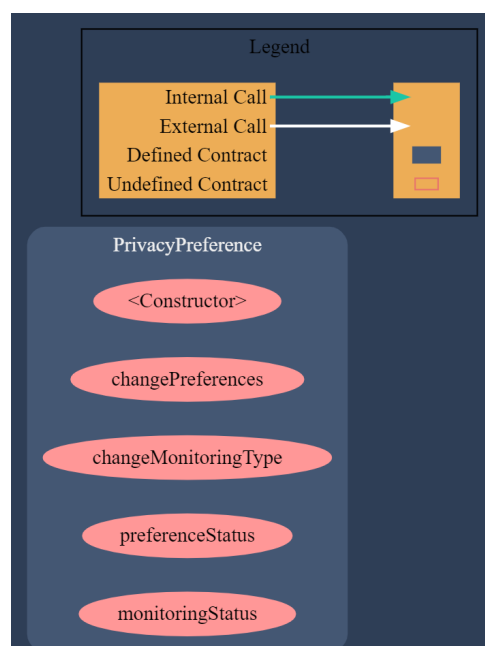
**Table 8.** DoS probability in relation to contract complexity.

Complexity	Probability of DoS
$O(1)$	Impossible
$O(n)$	High
$O(n^2)$	Extremely high
$O(2^n)$	Extremely high
$O(n!)$	Extremely high

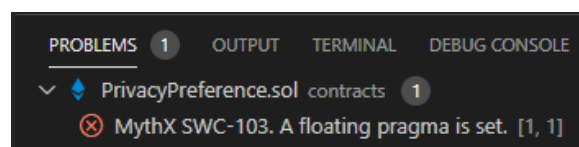
We used the Surya tool to generate a graphic representation of the contract developed and illustrate its complexity. Surya is a utility tool for smart contract systems that provides a number of visual outputs and information about the structure of the contracts. It also supports querying the function call graph for manual inspection of contracts. As shown in Figure 7, the contract functions do not interact with each other and cannot be called externally by other smart contracts. This approach reduces the complexity of contracts and avoids security issues.

As the last experiment, we used the audit tool Mythril to assess the security of the developed smart contract. Mythril is a security analysis tool for Ethereum Virtual Machine bytecode. It detects security vulnerabilities in smart contracts built and uses symbolic execution and Satisfiability Modulo Theories (SMTs) solving and taint analysis to detect a variety of security vulnerabilities. This tool searches for pieces of code that could lead to security inconsistencies and can detect vulnerabilities in smart contracts for Ethereum and other platforms. Figure 8 presents a screenshot of the report generated by Mythril showing the result obtained.

The report produced by the Mythril tool displays the security warning MythX SWC-103. A floating pragma is set, which is issued when we denote in the contract a different version of the pragma used in the compiler. The developed contract was built using version 0.6.4 (line 1 of Figure 3), while the Solidity compiler installed on the computer applied in the tests used version 0.6.7. This type of approach can be harmful as outdated versions of the pragma can generate bugs in the execution of the contract. To solve this problem, we need to change the contract to use the same version of the compiler installed on the machine.



**Figure 7.** Smart Contract Graph created using Surya tool.



**Figure 8.** Mythril analysis result.

## 7. Conclusions

This work presented a state-of-the-art storage architecture to guarantee privacy in license plate recognition systems. The architecture uses a private blockchain in conjunction with smart contracts and anonymization through ECC.

For this work, we conducted a review of the state-of-the-art solutions to provide privacy in platforms for the Internet of Things. The study demonstrated the lack of solutions to guarantee privacy in LPR systems and characterized the solutions currently developed for other IoT scenarios. In view of this, our work seems to be the first one to propose a solution to provide privacy in LPR systems using blockchain.

The results obtained confirmed the feasibility of implementing the proposed architecture. However, according to the tests performed, it is necessary to use sidechains for each state/city to maintain satisfactory network performance. Using only one blockchain to store all vehicle license plates of a country would make the system impracticable to be implemented because of performance and scalability issues.

The security analysis developed showed that the implemented smart contract is resistant to several types of attack. The approach used in this work to develop a contract of simple complexity favored the proposed architecture on security issues. However, it is necessary to emphasize that more complex architectures may need more complex contracts. In such cases, it is necessary to carry out a deeper security analysis in order to identify vulnerabilities that could compromise the proper functioning of the contract.

The analysis made in this article is an evolution of our previous work [6]. In addition to further detailing the proposed architecture and evaluating its performance, we seek to highlight the security of the developed architecture, focusing solely on the structure of smart contracts. In this way, we demonstrate the feasibility of implementing the proposed architecture through results obtained in performance and safety tests.

The solution proposed in this work is not restricted to LPR systems. Considering state-of-the-art technologies and platforms, anyone can adapt the proposed architecture to

other environments that need privacy, security, and trust in IoT scenarios. Blockchains have been widely used in IoT environments to ensure the operation of these systems. Thus, the results obtained also contribute to other researches that are being carried out in this area.

As future work, we intend to evaluate the proposed solution in other blockchain architectures aimed at IoT scenarios because, as mentioned in [48], the lack of a standard for analysis standard and requirements engineering is the main reason that drives blockchain to failure. We also intend to implement and evaluate the proposed architecture on other blockchain platforms for use in LPR systems, thus seeking to identify which platform is the most efficient to be used in this application. Besides, we intend to implement different levels of security and encryption, and develop security tests focused on the application gateway.

**Author Contributions:** Conceptualization, I.S.O., L.C., C.A.Z., and V.R.Q.L.; methodology, I.S.O., L.C., and V.R.Q.L.; software, I.S.O., V.R.Q.L., and L.C.; validation, I.S.O. and L.C.; writing—original draft preparation, I.S.O., L.C., V.R.Q.L., and C.A.Z.; writing—review and editing, J.F.D.P.S., W.D.P., L.O.S., C.A.Z., and V.R.Q.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Brasília, Brazil [Finance Code 001], Fundação de Amparo à Pesquisa de Santa Catarina (FAPESC), Florianópolis, Brazil [grant number 2019TR169], Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) [grants number 315287/2018-7 and 436982/2018-8], the Spanish Agencia Estatal de Investigación. Project Monitoring and tracking systems for the improvement of intelligent mobility and behavior analysis (SiMoMIAC). PID2019-108883RB-C21 / AEI / 10.13039/501100011033, and Fundação para a Ciência e a Tecnologia under Project UIDB/04111/2020.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Acknowledgments:** Seed Funding ILIND—Instituto Lusófono de Investigação e Desenvolvimento, COPELABS [COFAC/ILIND/COPELABS 2020]. Proyecto Uso de algoritmos y protocolos de comunicación en dispositivos con énfasis en la privacidad de los datos and Laboratório de Telecomunicações de Portugal IT—Branch Universidade da Beira Interior, Covilhã.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

CA	California
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
EFF	Electronic Frontier Foundation
EU	European Union
EVM	Ethereum Virtual Machine
FCPD	Fairfax County Police Department
GDPR	General Data Protection Regulation
IACP	Association of Chiefs of Police
IoT	Internet of Things
LPR	License Plate Recognition
SMT	Satisfiability Modulo Theory
UK	United Kingdom
US	United States

## References

1. Koreshoff, T.L.; Robertson, T.; Leong, T.W. Internet of things: A review of literature and products. In Proceedings of the 25th Australian Computer-Human Interaction Conference on Augmentation, Application, Innovation, Collaboration—OzCHI 13, Adelaide, Australia, 25–29 November 2013. [\[CrossRef\]](#)
2. Harrison, C.; Eckman, B.; Hamilton, R.; Hartswick, P.; Kalagnanam, J.; Paraszczak, J.; Williams, P. Foundations for Smarter Cities. *IBM J. Res. Dev.* **2010**, *54*, 1–16. [\[CrossRef\]](#)



3. Rjab, A.B.; Mellouli, S. Smart cities in the era of artificial intelligence and internet of things. In Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age, Delft, The Netherlands, 30 May 2018–1 June 2018; ACM Press: New York, NY, USA, 2018; pp. 81:1–81:10. [\[CrossRef\]](#)
4. Lum, C.; Koper, C.S.; Willis, J.; Happeny, S.; Vovak, H.; Nichols, J. The rapid diffusion of license plate readers in US law enforcement agencies. *Policing Int. J.* **2018**. [\[CrossRef\]](#)
5. American Civil Liberties Unions. You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements. 2019. Available online: <https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked> (accessed on 10 May 2019).
6. Ochôa, I.; Calbusch, L.; Viecelli, K.; de Paz, J.; Leithardt, V.; Zeferino, C. Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems Using Blockchain. In Proceedings of the 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019; pp. 1–5.
7. Du, S.; Ibrahim, M.; Shehata, M.; Badawy, W. Automatic License Plate Recognition (ALPR): A State-of-the-Art Review. *IEEE Trans. Circuits Syst. Video Technol.* **2013**, *23*, 311–325. [\[CrossRef\]](#)
8. UK Home Office. Automatic Number Plate Recognition. 2019. Available online: <https://www.gov.uk/government/publications/national-anpr-standards> (accessed on 10 May 2019).
9. CNN. Policing Advocates Defend Use of High-Tech License Plate Readers. 2013. Available online: <https://edition.cnn.com/2013/07/18/us/license-plate-readers/index.html> (accessed on 10 May 2019).
10. UK Home Office. Automatic Number Plate Recognition (ANPR) Strategy. 2016. Available online: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/909024/ANPR\\_-\\_Evaluation\\_Approved\\_Version\\_2.0.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909024/ANPR_-_Evaluation_Approved_Version_2.0.pdf) (accessed on 10 May 2019).
11. International Association of Police Chiefs. Support for License Plate Reader Systems. 2007. Available online: <https://www.theiacp.org/projects/automated-license-plate-recognition> (accessed on 10 May 2019).
12. United States Department of Justice. *Law Enforcement Management and Administrative Statistics (LEMAS)*; United States Department of Justice: Washington, DC, USA, 2007. [\[CrossRef\]](#)
13. United States Department of Justice. *Law Enforcement Management and Administrative Statistics (LEMAS)*; United States Department of Justice: Washington, DC, USA, 2013. [\[CrossRef\]](#)
14. The Electronic Frontier Foundation. Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers. 2018. Available online: <https://www.eff.org/pages/automated-license-plate-reader-dataset> (accessed on 10 May 2019).
15. Gierlack, K.; Williams, S.; LaTourrette, T.; Anderson, J.M.; Mayer, L.A.; Zmud, J. *License Plate Readers for Law Enforcement: Opportunities and Obstacles*; Rand: Santa Monica, CA, USA, 2014. Available online: [https://www.rand.org/pubs/research\\_reports/RR467.html](https://www.rand.org/pubs/research_reports/RR467.html) (accessed on 10 May 2019).
16. European Parliament. Regulation (EU) 2016/679 of the European Parliament. 2016. Available online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed on 10 May 2019).
17. EU. Art. 23 GDPR—Restrictions. 2019. Available online: <https://www.privacy-regulation.eu/en/article-23-restrictions-GDPR.htm> (accessed on 10 May 2019).
18. Boyne, S.M. Data Protection in the United States. *Am. J. Comp. Law* **2018**, *66*, 299–343. [\[CrossRef\]](#)
19. Police Collecting Databases of Vehicle Information. *Neil v. Fairfax County Police Department*; (v. Record No. 170247); Court of Fairfax County: Fairfax, VA, USA, 2018; p. 14;
20. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [\[CrossRef\]](#)
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 10 May 2019).
22. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18. [\[CrossRef\]](#)
23. Pouraghily, A.; Islam, M.N.; Kundu, S.; Wolf, T. Poster Abstract: Privacy in Blockchain-Enabled IoT Devices. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 17–20 April 2018; pp. 292–293. [\[CrossRef\]](#)
24. Rifi, N.; Rachkidi, E.; Agoulmine, N.; Taher, N.C. Towards using blockchain technology for IoT data access protection. In Proceedings of the 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), Salamanca, Spain, 12–15 September 2017; pp. 1–5. [\[CrossRef\]](#)
25. Cha, S.; Tsai, T.; Peng, W.; Huang, T.; Hsu, T. Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. In Proceedings of the 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 24–27 October 2017; pp. 1–3. [\[CrossRef\]](#)
26. Pinno, O.J.A.; Gregio, A.R.A.; De Bona, L.C.E. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6. [\[CrossRef\]](#)

27. Huang, Z.; Su, X.; Zhang, Y.; Shi, C.; Zhang, H.; Xie, L. A decentralized solution for IoT data trusted exchange based-on blockchain. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 1180–1184. [\[CrossRef\]](#)
28. Dang, T.L.N.; Nguyen, M.S. An Approach to Data Privacy in Smart Home using Blockchain Technology. In Proceedings of the 2018 International Conference on Advanced Computing and Applications (ACOMP), Ho Chi Minh City, Vietnam, 28–30 November 2018; pp. 58–64. [\[CrossRef\]](#)
29. Ayoade, G.; Karande, V.; Khan, L.; Hamlen, K. Decentralized IoT Data Management Using Blockchain and Trusted Execution Environment. In Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, 7–9 July 2018; pp. 15–22. [\[CrossRef\]](#)
30. Paul, R.; Baidya, P.; Sau, S.; Maity, K.; Maity, S.; Mandal, S.B. IoT Based Secure Smart City Architecture Using Blockchain. In Proceedings of the 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), ChangSha, China, 21–23 September 2018; pp. 215–220. [\[CrossRef\]](#)
31. Gallo, P.; Pongnumkul, S.; Quoc Nguyen, U. BlockSee: Blockchain for IoT Video Surveillance in Smart Cities. In Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I CPS Europe), Palermo, Italy, 12–15 June 2018; pp. 1–6. [\[CrossRef\]](#)
32. Le, T.; Mutka, M.W. CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Sicily, Italy, 18–20 June 2018; pp. 57–64. [\[CrossRef\]](#)
33. Liang, X.; Zhao, J.; Shetty, S.; Li, D. Towards data assurance and resilience in IoT using blockchain. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 261–266. [\[CrossRef\]](#)
34. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized Blockchain for IoT. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
35. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access* **2018**, *6*, 17545–17556. [\[CrossRef\]](#)
36. Ali, M.S.; Dolui, K.; Antonelli, F. IoT Data Privacy via Blockchains and IPFS. In *IoT '17: Proceedings of the Seventh International Conference on the Internet of Things*; ACM: New York, NY, USA, 2017; pp. 14:1–14:7. [\[CrossRef\]](#)
37. Chanson, M.; Bogner, A.; Wortmann, F.; Fleisch, E. Blockchain As a Privacy Enabler: An Odometer Fraud Prevention System. In *UbiComp '17: Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*; ACM: New York, NY, USA, 2017; pp. 13–16. [\[CrossRef\]](#)
38. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, D. Providing Privacy, Safety, and Security in IoT-based Transactive Energy Systems Using Distributed Ledgers. In *IoT '17: Proceedings of the Seventh International Conference on the Internet of Things*; ACM: New York, NY, USA, 2017; pp. 13:1–13:8. [\[CrossRef\]](#)
39. Le, D.; Meng, H.; Su, L.; Yeo, S.L.; Thing, V. BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy. In Proceedings of the TENCON 2018—2018 IEEE Region 10 Conference, Jeju Island, Korea, 28–31 October 2018; pp. 2372–2377. [\[CrossRef\]](#)
40. Loukil, F.; Ghedira-Guegan, C.; Boukadi, K.; Benharkat, A.N. Towards an End-to-End IoT Data Privacy-Preserving Framework Using Blockchain Technology. In *Web Information Systems Engineering—WISE 2018*; Hacid, H., Cellary, W., Wang, H., Paik, H.Y., Zhou, R., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 68–78. [\[CrossRef\]](#)
41. Yang, M.; Zhu, T.; Liang, K.; Zhou, W.; Deng, R.H. A blockchain-based location privacy-preserving crowdsensing system. *Future Gener. Comput. Syst.* **2019**, *94*, 408–418. [\[CrossRef\]](#)
42. Andreica, T.; Groza, B. Secure V2V Communication with Identity-based Cryptography from License Plate Recognition. In Proceedings of the 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019, Granada, Spain, 22–25 October 2019; pp. 366–373. [\[CrossRef\]](#)
43. Baig, M.I.; Shuib, L.; Yadegaridehkordi, E. Big data adoption: State of the art and research challenges. *Inf. Process. Manag.* **2019**, *56*, 102095. [\[CrossRef\]](#)
44. Lucca, A.V.; Sborz, G.A.M.; Leithardt, V.R.Q.; Beko, M.; Zeferino, C.A.; Parreira, W.D. A Review of Techniques for Implementing Elliptic Curve Point Multiplication on Hardware. *J. Sens. Actuator Netw.* **2021**, *10*, 3. [\[CrossRef\]](#)
45. New York State Vehicle Registrations. Available online: <https://dmv.ny.gov/statistic/2017reginforce-web.pdf> (accessed on 10 May 2019).
46. Dika, A.; Nowostawski, M. Security Vulnerabilities in Ethereum Smart Contracts. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 955–962. [\[CrossRef\]](#)

- 
47. Saad, M.; Njilla, L.; Kamhoua, C.; Kim, J.; Nyang, D.; Mohaisen, A. Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 285–292. [\[CrossRef\]](#)
  48. Drljevic, N.; Aranda, D.A.; Stantchev, V. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Comput. Stand. Interfaces* **2020**, *69*, 103409. [\[CrossRef\]](#)